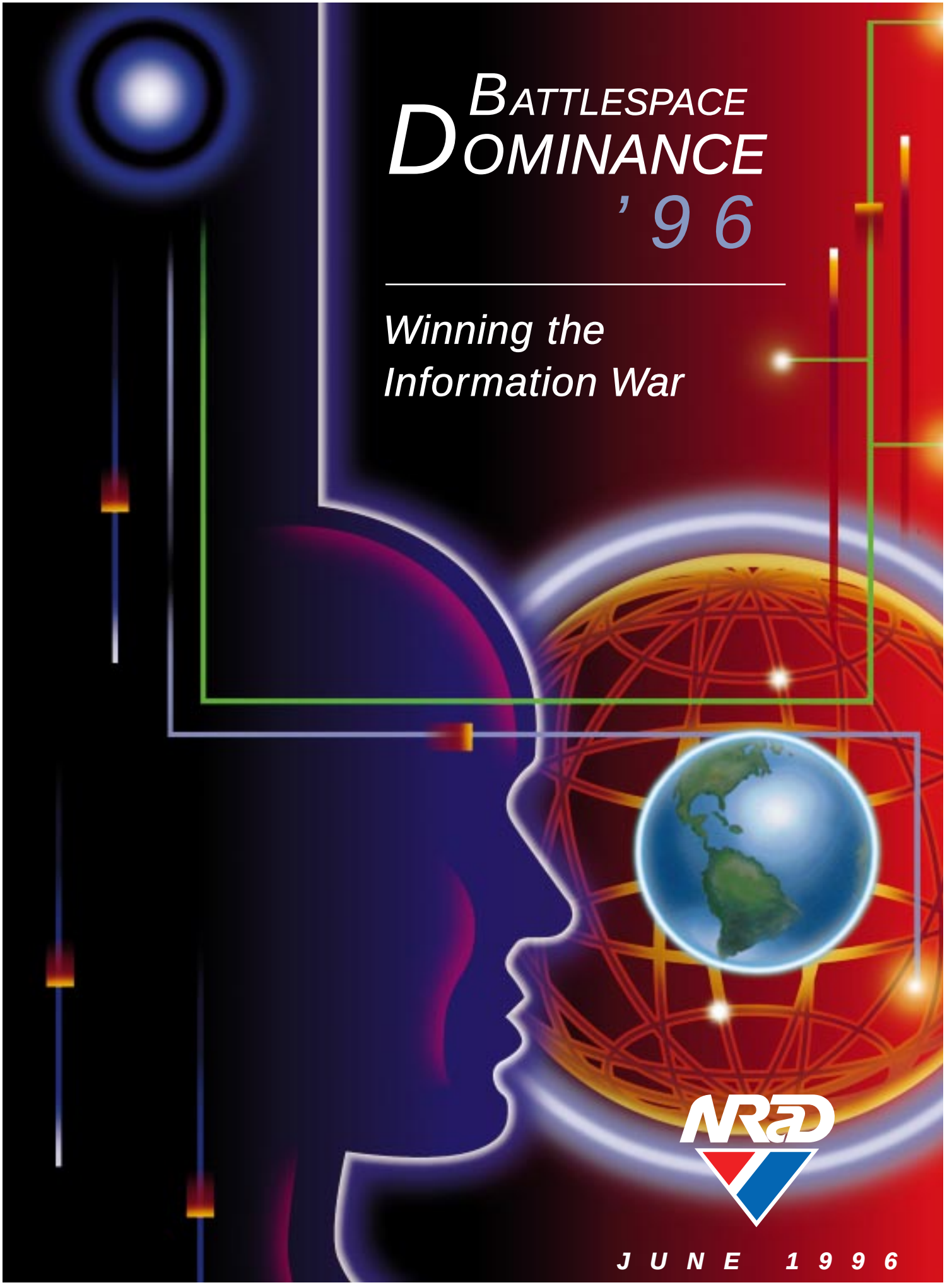
BATTLESPACE DOMINANCE '96

Winning the Information War



NRaD

JUNE 1996

Making information dominance for the warrior a reality

BATTLESPACE DOMINANCE '96

Winning the Information War

"To fight and conquer in all our battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting."

— Sun Tsu, The Art of War

"We are in the midst of a time of significant change that is no less revolutionary than the advent of steam propulsion, carrier aviation or nuclear submarines. The Revolution in Military Affairs has moved information and the requirement for information dominance in the joint battlespace to center stage in our thinking about modern warfare."

— ADM J. M. Boorda

JUNE 1996

Information Dominance

Information in Military Operations

A revolution in military affairs has moved information dominance in military operations to center stage. Along with diplomatic skills and economic and military strength, information dominance is now one of the four primary instruments of national power. A nation that is able to affect an adversary's information can employ information as a powerful weapon. By shaping information available to an opponent and by protecting our own information, we can influence an opponent's military behavior. By leveraging our nation's advantages in the field of information, U.S. forces can stay a step ahead of potential adversaries and perhaps deter combat altogether.

Information has always affected the outcome of warfare. As the Gulf War showed, information and the capability to use it have become more important to modern warfare than strength of numbers or defensive positions. Information allowed the U.S. and its allies to outflank the Iraqis and to operate within the Iraqi decision-cycle time, giving an immense tactical advantage.

Conversely, lack of information left Iraqi forces with few tactical options and little capability to evaluate those options. And lack of information on deployment of Iraqi mines denied a superior U.S. Navy–Marine Corps force the opportunity to conduct effective amphibious operations in the Gulf. In many ways, the dominance of information in warfare has become a key factor in the military outcome.

As Wayne Hughes, Jr., states in his book *Fleet Tactics*, written before Desert Storm:

> "As the potential for sudden, coordinated shock attack grows, and that is the obvious trend, the roles of C^2 and of countermeasures against the enemy's C^2 take on new and compelling significance. A modern tactical commander will expend relatively less of his energy on planning for and delivering firepower, and relatively more on planning and executing his scouting effort and forestalling that of the enemy with antiscouting and C^2 countermeasures."

Information is key to effective military operations. Information dominance, then, is *providing the warrior sufficient and timely information and associated tools to plan and execute effectively, while denying—through both active and passive means—the enemy adequate information on which to plan and execute effectively*. Information dominance is central to modern warfare—it can create a military advantage as tactically significant as numerical end strength.

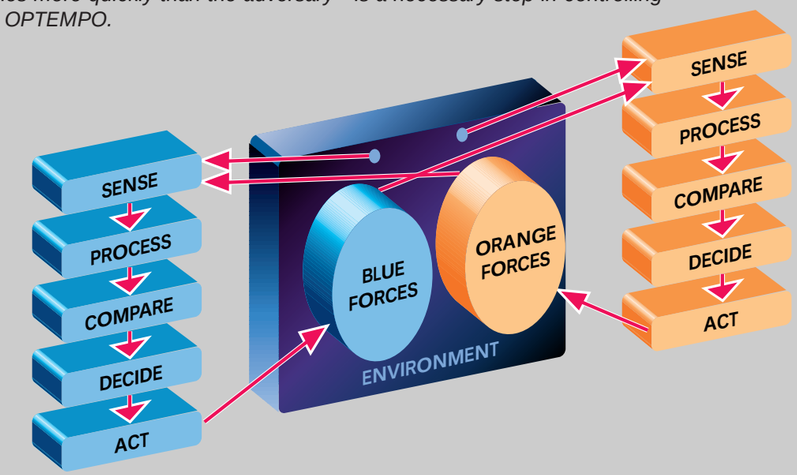
The C^4I Decision Cycle

In the late 1970s, Dr. Joel Lawson, then Technical Director of the Naval Electronic Systems Command, devised a sketch of the command process as it applies to military forces. A simplified version of his concept for two opposing forces is shown in the accompanying diagram. The diagram suggests two command "cycles," one executed by blue and one by orange.

Each side performs a sensing function to "sample" the "system" (composed of the environment, the opposing forces, and neutral elements in an area of interest), gathering information on natural factors such as terrain and weather, and on all aspects of friendly, neutral, and hostile or potentially hostile elements. Next, the various sensor outputs are combined with other available information to form a perception of the current situation. This perceived state is then compared with a desired state as established by higher authority. The results of the comparison are inputs to a decision process in which alternative courses of action intended to alter (or perhaps maintain) the state are evaluated, and a course of action selected. Finally, actions are taken which direct forces (and sensors). The actions alter the state of the system, and the cycle is then repeated.

Clearly this is not a simple feedback control process, since both blue and orange are attempting to alter the system state in their favor. The time to execute the command control cycle becomes critical in any warfare situation. It is highly desirable for blue to be able to manipulate the system more quickly than orange can respond, so that orange's decisions, based on poor information, are also poor—that is, benefiting blue. This implies that quality is a factor in the cycle time. The objective in terms of decision-cycle time is to execute a high-quality cycle—one that brings the system closer to the desired state—quickly.

A primary goal of command is to control the tempo of operations. Initiative in battle rests with the commander who controls the "OPTEMPO"; he will call the shots and force his adversary into a reactive mode. Acting "inside" the adversary's decision cycle—executing high-quality cycles more quickly than the adversary—is a necessary step in controlling the OPTEMPO.

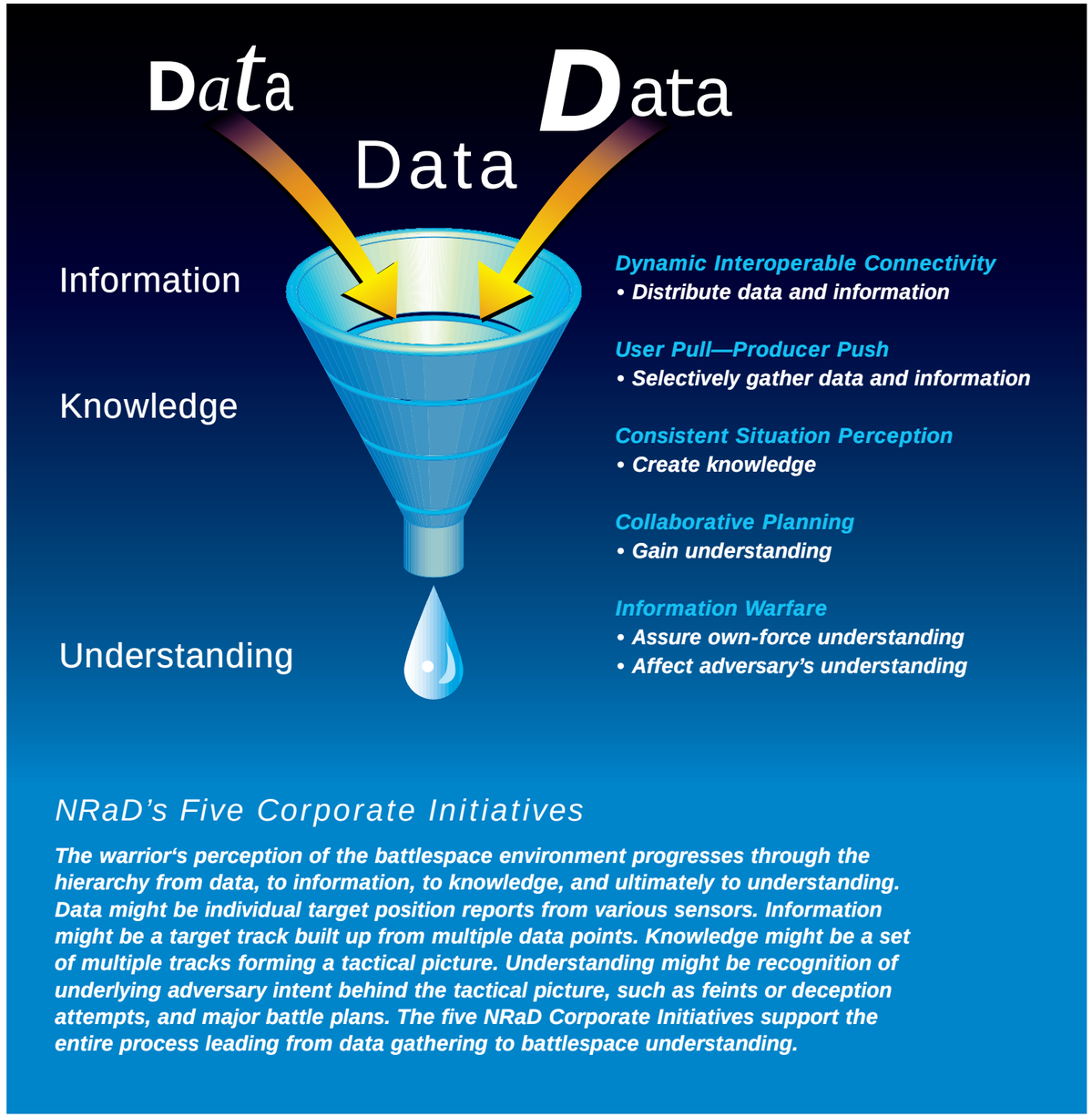


NRaD's Role—Providing Tools for Achieving Information Dominance

NRaD is uniquely qualified to provide the expertise and tools to achieve information dominance. Almost every NRaD effort deals with acquiring data, transforming data into information, using information to operate, or moving data and information from where they reside to where they are needed. NRaD is involved in every aspect of the processes of transforming data into information into knowledge into understanding. NRaD's great strength is its unique work across the spectrum of C4I and surveillance. This work ranges from basic research to life-cycle support of fielded systems, and from prototyping to fully produced systems. NRaD is applying these capabilities to the central element of future naval warfare—information dominance.

NRaD's Vision—The Initiatives

NRaD's vision—making information dominance for the warrior a reality—is based on achieving five interrelated objectives, or Corporate Initiatives. Our first initiative, Dynamic Interoperable Connectivity, will provide assured, user-transparent connectivity, on demand, to any desired location in the "infosphere," the worldwide grid of military databases, fusion centers, national resources, and commercial information. Given this fundamental capability, our second initiative, User Pull/Producer Push, will use that connectivity to access strategically located database servers and anchor desks and provide users, at all levels, with the key information needed to create and share a consistent perception of the operational situation. Achieving Consistent Situation Perception is our third initiative. When all key operational commanders have a consistent tactical understanding, tools supporting our fourth initiative, Collaborative Planning, can be used to collaboratively plan and execute time-critical missions and tasks. Our fifth initiative, Information Warfare, will protect our information resources while denying our enemy the information needed to implement aggressive actions.



NRaD's Five Corporate Initiatives

The warrior's perception of the battlespace environment progresses through the hierarchy from data, to information, to knowledge, and ultimately to understanding. Data might be individual target position reports from various sensors. Information might be a target track built up from multiple data points. Knowledge might be a set of multiple tracks forming a tactical picture. Understanding might be recognition of underlying adversary intent behind the tactical picture, such as feints or deception attempts, and major battle plans. The five NRaD Corporate Initiatives support the entire process leading from data gathering to battlespace understanding.

Interrelationships Among the Initiatives

Requirements for command and control (C^2) of specific forces derive from the roles and missions assigned to those forces, the force composition, force capabilities, and operational doctrine. Operational C^2 depends on an underlying command structure. To support operational C^2, our system capabilities must span the entire range of roles, missions, organizational structures, and politics, or any subset of these. The five NRaD Corporate Initiatives form the core capability for information dominance.

Because the battlespace is undersampled in both space and time, shared data from multiple sources must be fused into information. As enhanced communications allow common sharing of that information, all warriors can collaboratively determine the best estimate of current events and status, forming a Consistent Situation Perception.

User Pull/Producer Push impacts, and is impacted by, Dynamic Interoperable Connectivity. To make User Pull/Producer Push achievable, the communications infrastructure must:

- Allow interoperability among all components of a force;
- Allow every force unit to interact with the infosphere;
- Support guaranteed information delivery with automatic forwarding (for "pushes" or "pulls"), or, in case of failure, notification of inability to deliver;
- Provide adequate throughput for required information.

User Pull/Producer Push enables Collaborative Planning and synchronized execution. The ability to support information access will be key to successful implementation of these two critical areas. Two external processes support planning and execution: situation assessment (with status assesssment of actual vs. planned execution) and information management. The latter process is "user pull" and is primarily an information feed to the planning capabilities. User Pull/Producer Push provides information access needed to develop a Consistent Situation Perception.

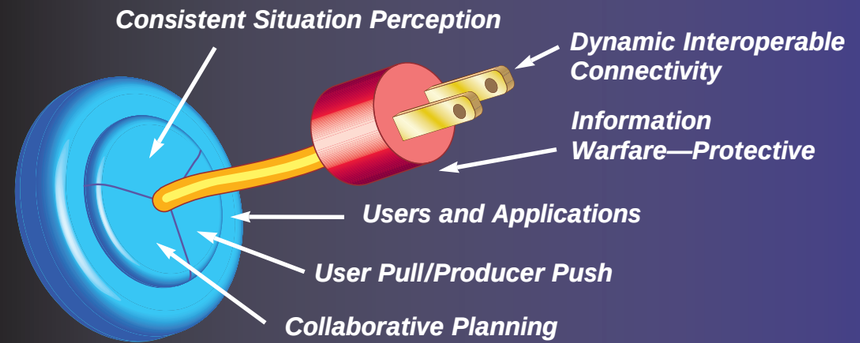
The Corporate Initiatives are interdependent—all five are required *as a set* in order to provide the operational command with tools needed for successful C^2.

- Without Dynamic Interoperable Connectivity, User Pull/Producer Push is not ensured.
- Without User Pull/Producer Push, Consistent Situation Perception within a defined battlespace cannot be achieved.
- Without the first three initiatives, Collaborative Planning and replanning of operations cannot take place, nor can those plans be executed in time synchronization.
- Without protective Information Warfare, these capabilities and our ability to perform C^2 can be lost.

A distinction must be made between satisfying the five initiatives to support effective C^2 and ensuring mission operational success. Without satisfying the initiatives, effective C^2 is impossible. However, satisfying the initiatives in no way ensures effective C^2. Good systems do not turn poor commanders into excellent ones. As long as military operations depend on human judgment, intuition, "seaman's eye," a "feel for combat," and accurate prediction of enemy behavior, C^2 systems will play only a support role in naval or joint operations. The Corporate Initiatives are like the five senses—they allow us to interact with our environment. But they do not ensure individual success in dealing with it. Success requires cognition, value judgments, philosophy, and a little luck. So it is with C^2.

The five NRaD Corporate Initiatives are necessary conditions for effective C^2, regardless of scenario.

Information Dominance at a Single Navy Node



The outer ring of users and applications (including offensive information warfare) access the supporting mechanisms of User Pull/Producer Push, Consistent Situation Perception, and Collaborative Planning. These mechanisms in turn access the infosphere through Dynamic Interoperable Connectivity. Protective Information Warfare defends the entire information system from hostile access and exploitation. The users and applications may then build on these five areas to support mission planning, preparation, and execution. Offensive information warfare behaves like other users and applications, accessing the infosphere through the information dominance ring structure. The applications are specific decision support tools that reside within the modular structure of the overall C^2 system.

NRaD Corporate Initiatives

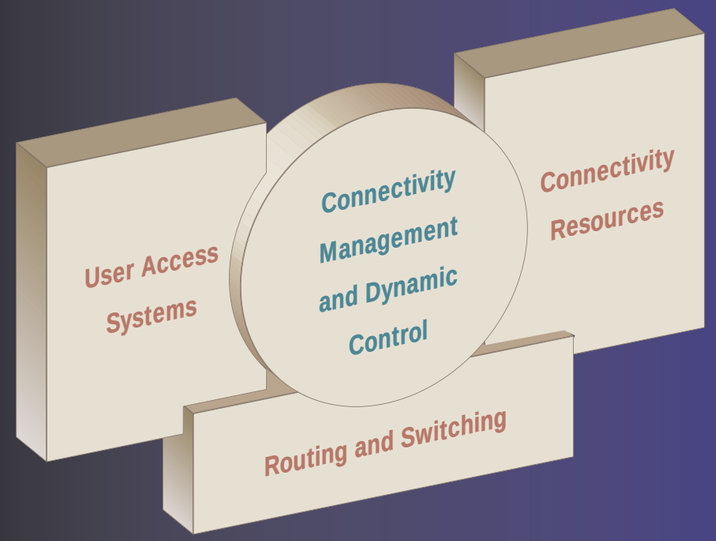
Dynamic Interoperable Connectivity

Dynamic Interoperable Connectivity is the conduit for all data and information, whether that information moves 15 feet or 15,000 miles. The Dynamic Interoperable Connectivity initiative aims to ensure that the warrior has reliable and secure access to all needed information. Providing worldwide user pull/producer push requires an integrated global network for gathering and exchanging information. This includes extensive high-capacity landline connections among military users to maintain extensive databases from which warriors may "pull." It also requires improved in-theater communications for better response to the warrior's needs, particularly the dynamic movement of imagery and large files among warriors—a requirement that would overwhelm existing low-capacity radio links.

Timely information availability is critical to command and warfighting processes. The methods of information sharing—what is needed and when it is needed—are determined by the user. Therefore, users must control connectivity. This is analogous to the telephone system. Telephone users themselves determine who they wish to connect to and when, connect by dialing, then disconnect when done. Self-determined connectivity will also apply in the military environment.

Not all connectivity users are people. Machines also must exchange data. Connectivity supporting machine data exchange has been accepted Navy practice for the three decades since the introduction of the Naval Tactical Data System and Link 11. Connectivity can involve any number of people and machines, in various locations, as required to accomplish a task.

Connectivity, then, is a mechanism supporting information transfer. The command structure normally, though not always, assumes that connectivity exists between superior and subordinate, and also usually peer-to-peer. While connectivity is needed to support both access and command, the "flow" may differ in the two cases. In particular, information access is generally thought to be best supported by "user pull," while command is best supported by "producer push." That is, in information access (user pull) the information user is seeking something and requests it, while in command access (producer push) the information originator wants to "tell" something (issue an order, ask for authority, etc.). Dynamic Interoperable Connectivity must support both user pull and producer push concepts for information access, as well as command and impromptu person-to-person interaction.



A Top-Level Nodal View of Dynamic Interoperable Connectivity

User access systems are the interfaces for connecting users to other users and systems. The interfaces might include telephone handsets, video conferencing devices, and input/output schemes including keyboards, touch pads, track balls, mice, and various display technologies. Routing and switching connects the user access systems to one another and to the various off-node connectivity resources. Connectivity resources include radio links, wireline, and fiber optics, and possibly acoustic systems. Connectivity management and dynamic control determines how to most effectively meet the real-time connectivity needs of the user systems within the constraints of current connectivity resources and command-established priorities.

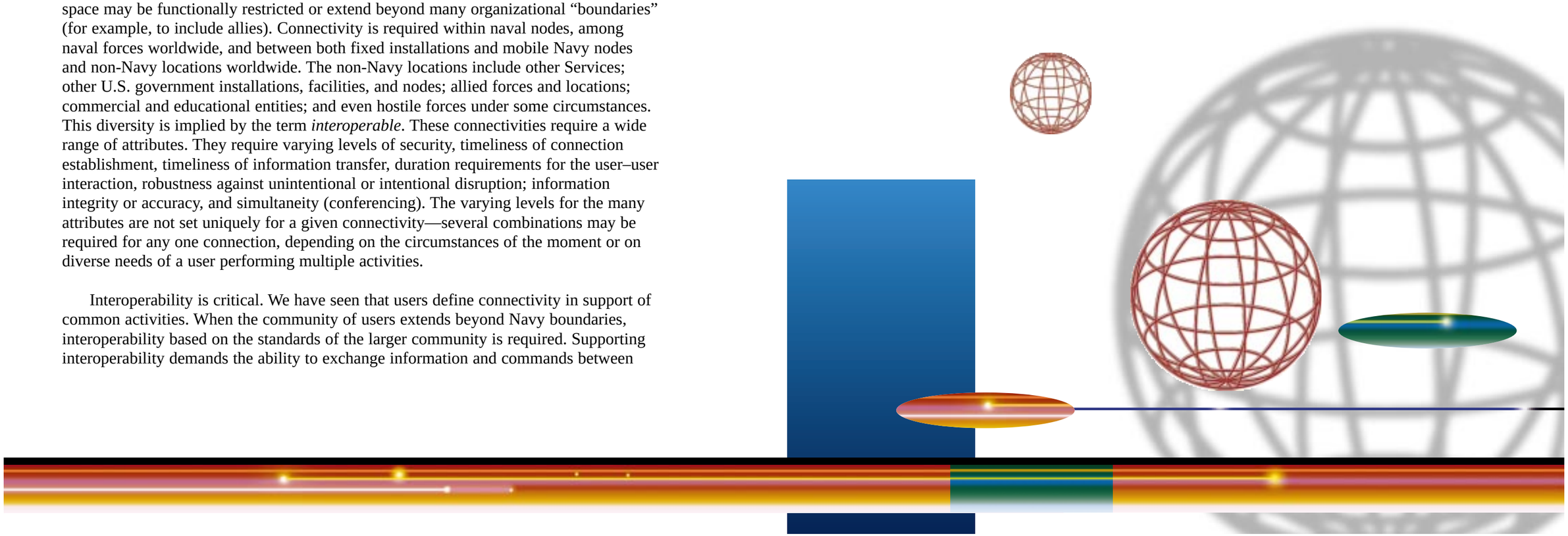
Dynamic connectivity is flexible, supporting the time-varying needs of users. But it is also economic, supporting the sharing of resources. Again the telephone is a useful analogy. Telephone connections are dynamic, with all resources, from user handsets through physical links and central switches, shared among many users. This allows a given set of resources to serve many times the needs that could be supported by static connections. In addition, individual users generally perform many functions and belong to multiple user communities associated with those functions. The functions may each require only part-time involvement. Connectivity requirements will then track the shifting task involvements.

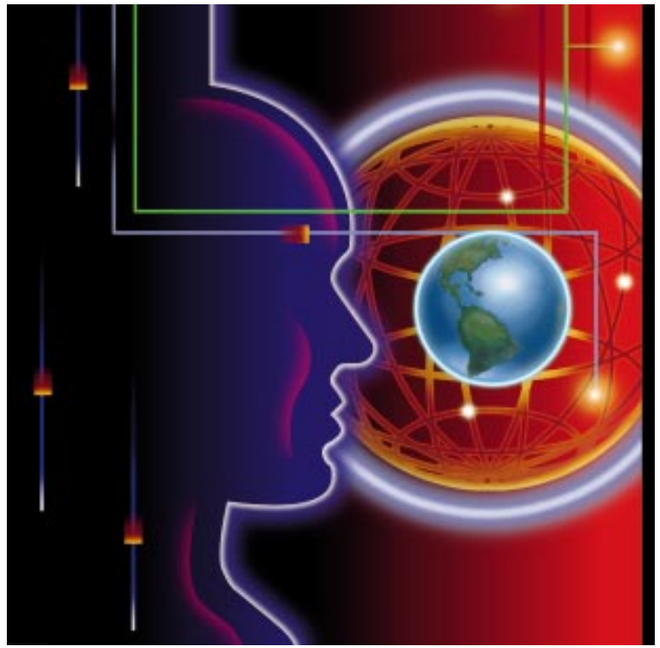
Dynamic Interoperable Connectivity is defined by a community of users, not by distances or physical communications media. It might involve two users in adjacent offices or compartments connected by copper wire (perhaps a person operating a workstation, and a database), or it might involve many users throughout a region working on a common problem connected by a mix of submarine fiber optics, wire lines, and satellite radio links—for example, a group of sensors, processing algorithms, databases, and analysts tracking surface ships in the Pacific.

Both access and command span the user's "operational" space. The operational space may be physically small, or global, depending on the user's role. The operational space may be functionally restricted or extend beyond many organizational "boundaries" (for example, to include allies). Connectivity is required within naval nodes, among naval forces worldwide, and between both fixed installations and mobile Navy nodes and non-Navy locations worldwide. The non-Navy locations include other Services; other U.S. government installations, facilities, and nodes; allied forces and locations; commercial and educational entities; and even hostile forces under some circumstances. This diversity is implied by the term *interoperable*. These connectivities require a wide range of attributes. They require varying levels of security, timeliness of connection establishment, timeliness of information transfer, duration requirements for the user–user interaction, robustness against unintentional or intentional disruption; information integrity or accuracy, and simultaneity (conferencing). The varying levels for the many attributes are not set uniquely for a given connectivity—several combinations may be required for any one connection, depending on the circumstances of the moment or on diverse needs of a user performing multiple activities.

Interoperability is critical. We have seen that users define connectivity in support of common activities. When the community of users extends beyond Navy boundaries, interoperability based on the standards of the larger community is required. Supporting interoperability demands the ability to exchange information and commands between users. This in turn places demands on all of the underlying procedures, processes, and hardware at every level. Interoperability implies a common (human or machine) language, common security methods and shared "keys," common protocols, and common modulation formats or methods. Where these items are not shared in common, translation mechanisms must be provided.

Now and for the foreseeable future, the number of possible connections and the capacities of those connections between mobile nodes will fall short of total user demands. Therefore, the command organization will have to allocate available resources to users based on mission and operational needs. Some resources needed to support Dynamic Interoperable Connectivity are inherently limited. Spectrum must be shared among surveillance (both active and passive); navigation; identification, friend or foe; communications; command control warfare; and weapons systems (soft-kill systems, in-flight missile guidance). Physical space for radios is limited, and today's radio systems (cryptographic device, modem, transmitter/receiver, antenna coupler, antenna) are usually dedicated to a single user or group. A goal for Dynamic Interoperable Connectivity is to eliminate dedicated equipment and spectrum. Reducing dedication of equipment and spectrum to single users will increase efficiency, expand the number and types of users having communications access at any given time, and reduce costs.



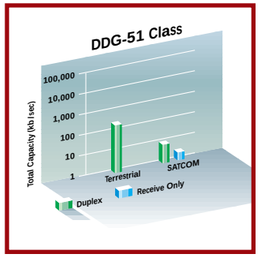


Now and for the foreseeable future, the number of possible connections and the capacities of those connections between mobile nodes will fall short of total user demands.

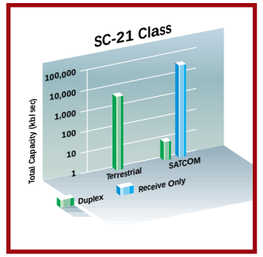
Dynamic Interoperable Connectivity Evolution

Today... Evolving to... → TOMORROW

Links and Networks

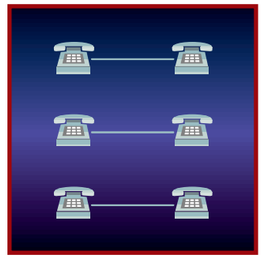


- Narrowband spectrum channelization
- Inflexible hardware
- Single-function radio equipment (antennas, radios, modems)
- Capacity at 1960s level
- Expeditionary warfare "user penetration" limited
- Military-unique systems



- Flexible spectrum channelization
- Programmable/controllable hardware (e.g.,Speakeasy)
- Shared apertures
- Capacity enhanced by 3+ orders of magnitude
- PCS/pager/cellular for the expeditionary warrior
- Exploiting commercial technology

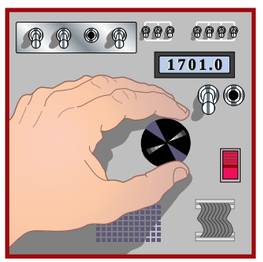
User Access/Connectivity



- Links dedicated to users
- Single-level security per user
- Push-to-talk voice network sharing
- Initial Internet Protocol packet service

- Links shared dynamically (capacity on demand)
- Multilevel secure access plus link encryption
- Multimedia (voice, data, video) integration
- Seamless asynchronous transfer mode user–user

Connectivity Management



- Manual patching, tuning, configuring
- Introducing "federated" commercial management software
- Independent management of voice and data

- Automated equipment monitoring and control
- Integrated management system (software)
- Management of integrated services
- Connectivity management integrated with total electromagnetic systems management

User Pull/Producer Push

A revolution in connectivity and distributed computer power is creating a potential for access to information that must be applied judiciously. User Pull/Producer Push describes the interactive processes for information producers and information users (warriors). The User Pull/Producer Push initiative focuses on the warrior's need for enough information to act appropriately, but not so much that confusion results. User pull is the "call for as needed" capability that allows the warrior to access information, only as needed, based on changes in the operational situation. This capability requires robust information servers to support database searching by forces deployed anywhere. Repositories of current, pertinent information, located at anchor desks, provide the warrior with access to seek and receive the right information at the right time.

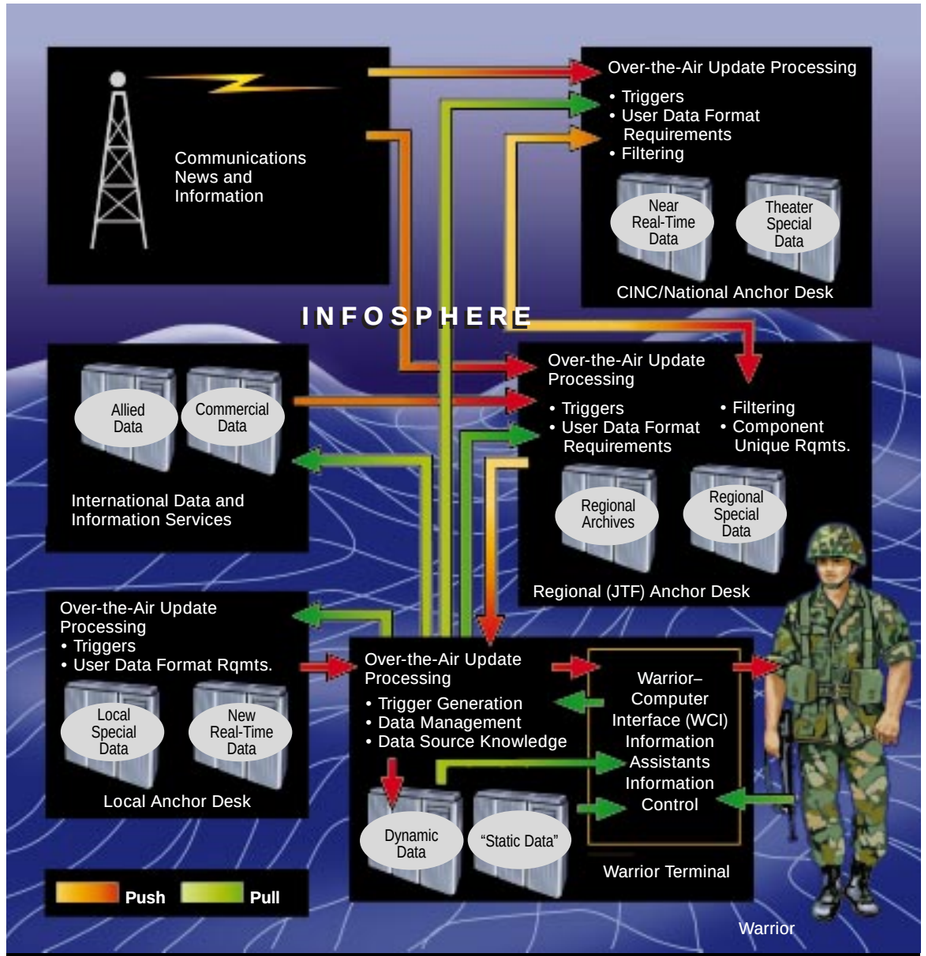
The User Pull/Producer Push initiative will develop ways to meet user information needs for C^2 at all levels. Warriors must be able to access the universe of information without the need for undue technical skills. The basic capabilities will consist of (1) user pull information transfer, (2) producer push, and (3) preplanned "information ordering."

User pull information transfer is a "call for as needed" capability allowing warriors dynamic access to information according to mission situations. Warriors of any rank will access the infosphere.

Producer push allows command centers to inform and direct warriors as needed, whenever warriors have insufficient knowledge or indications to formulate a request. Key to producer push is intelligent selection, or screening.

Preplanned information ordering has two components. First, preplanned essential information is assembled by the warrior (at any command level) before a mission. Preplanned essential information comes from existing databases, which may be fixed in the sense that they are built and maintained independently of any specific mission. Second, information is updated as the mission requires by over-the-air updating.

Supporting User Pull/Producer Push will be an improved information transfer infrastructure, allowing warriors to access the infosphere via warrior terminals and dynamically configurable anchor desks. The infrastructure will be an integrated architecture of seamless connectivity. The warrior terminals will use advanced human–system interface technologies to empower warriors, not divert them. Information transfer will be controlled, contrasting with the previous paradigm, a broadcast of uncontrolled traffic that stressed message delivery and often inundated warriors.



User Pull, Producer Push, the Warrior Terminal, and Anchor Desks

User pull information transfer is a "call for as needed" capability allowing warriors dynamic access to information according to mission situations. Producer push allows command centers to inform and direct warriors as needed. The warrior terminal accesses the infosphere as the primary means of gathering battlespace information, while anchor desks control information flow by organizing, developing, and distributing it. User pull, producer push, and the warrior terminal/anchor desk are inseparable—they must work together to provide the warrior with information access, control, and use.

The warrior terminal can have many configurations, for example a workstation at a desk or a mobile backpack unit. The warrior terminal has the necessary automatic data processing equipment to hold information (dynamic data and preplanned essential information) and to perform two basic functions: user interaction and over-the-air update processing.

User interaction is provided through (1) a warrior–computer interface, (2) information assistants, and (3) information control. The *warrior–computer interface* is broader in scope than a typical human–computer interface since the warrior terminal must allow use by an automaton (an information assistant) as well as by a human. The great volume of available information demands that warriors have support in browsing, cataloging, and making sense of information—we call such support *information assistants*. Assistants, which are basically computer programs, will use decision support algorithms and artificial intelligence to help process the volume and diversity of the infosphere. To control access to information (e.g., security clearances) and to "program" the producers of information on what to "push," the warrior–computer interface has *information control*.

Over-the-air update processing has three aspects: (1) trigger generation, (2) data management, and (3) data source knowledge. *Trigger generation* creates and distributes (to "pushers") "triggers," which are "information path rules ... that describe what, when, and how often the updates occur." The warrior terminal performs traditional *data management*, including storage and retrieval of information that is pulled or pushed. *Data source knowledge* tracks possible information sources and required intricacies of the infosphere to allow interaction with such sources.

Warriors need support in browsing, cataloging, and making sense of information—we call such support information assistants.

The warrior terminal accesses the infosphere as the primary means to gather battlespace information (though human data entry, such as manual tracking, is not ruled out). The infosphere includes (1) anchor desks, (2) information retrieval services (commercial or allied military), and (3) commercial news and information broadcasts.

Anchor desks control the flow by organizing, developing, and distributing information. Anchor desks vary with command level (local or component, Joint Task Force, theater) and function (command, support, special). Anchors at different command levels control the volume of information flow by defining a user's scope. Function-specific anchor desks control flow by information type. Anchor desks are highly connected in the infosphere and contain many information bases appropriate to the anchor desk's scope. Over-the-air update processing at anchor desks is similar to that of the end-use warrior terminal and involves four elements: (1) "triggers" created by warriors are executed (in "pushing"); (2) data are formatted optimally for transmission and consumption by warriors; (3) disparate information is filtered and fused according to expert operators/automatons; and (4) any unique needs by a component (e.g., a special operations force) are handled by appropriate human involvement.

Information retrieval services will be available to the warrior for pulling data. Commercial examples would be the World Wide Web or equity market systems such as Dow Jones. An example of an allied source of information would be allied members' libraries of text messages.

Commercial news and information broadcast services, such as CNN, are sources that push information at everyone through broadcasts. Information from these broadcasts can be analyzed at anchor desks and results pushed down to other warriors.

In summary, warriors "pull" information from the infosphere via anchor desks using warrior terminals with warrior–computer interface and information assistants. Information is "pushed" to warriors from anchor desks, incorporating information from services including commercial news broadcasts.

User Pull/Producer Push Evolution

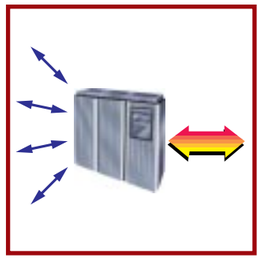
Today... Evolving to... → TOMORROW

The Warrior Terminal

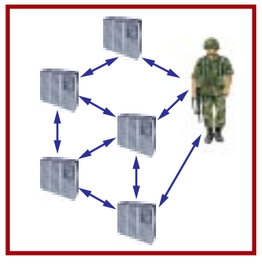
- JMCIS/Unified Build
- Information "pre-loads" on compact disk
- Pull from heterogeneous databases
- Anchor desk assistance
- Access to platform archives
- Warrior-controlled "triggers" for producer push
- Voice-video-data integration
- Embedded training

- Real-time terminal functionality reconfiguration
- 3-D and virtual reality displays
- Information access and assembly using knowledge "knowbots"
- Animated "what-if" analyses and real-time simulations

Anchor Desks



- Specific operational focus (e.g., logistics)
- Data and request format translations
- Filtering; "push" control
- Information access and retrieval assistance (e.g., maintaining detailed "web pages")
- Warrior "trigger" acceptance and implementation



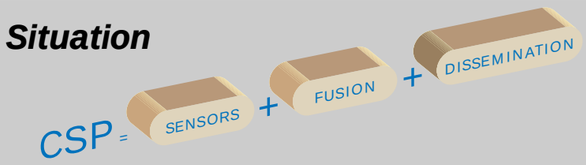
- Warrior-launched "knowledge robots"
- Object-oriented information structure
- Reduced/eliminated need for anchor desks

Consistent Situation Perception

The Consistent Situation Perception initiative focuses on developing a shared understanding of the "operational picture" across all command levels. This understanding is formed from diverse information types from the infosphere and from data sources within the theater. Because there are relatively few tactical platforms to gather data, autonomous sensors are needed to gather in-theater data. In addition to data, Consistent Situation Perception requires connectivity and display capabilities to enable collaborative discussions in order to place the data in its proper operational context.

Consistent Situation Perception develops information (location/identity/status/capabilities/intentions) on all assets (hostile/neutral/friendly) and the environment, within a given geographic area. Through information sharing and collaborative discussion among distributed users, Consistent Situation Perception is firmed into a common operational picture. Consistent Situation Perception is more than mere data collection. Sensed data, when logically fused with other data, intelligence, and background information, and then transcribed to a common vernacular, becomes the information for a singular view. Dissemination of the view (by local display or by communicating to remote users) and discussion among warriors with differing views lead to a common perception of the situation. Three elements—sensing, fusion, and dissemination—are needed to create Consistent Situation Perception.

Consistent Situation Perception



A shared, consistent perception of the situation among warriors at different commands and echelons of those commands results in common understanding. The challenge is to maintain a timely, consistent perception among distributed users as the operational situation evolves and as the availability of data changes.

The two fundamental Consistent Situation Perception objectives are to create a timely situation perception and to make it consistent and understandable at all levels within each user community. Consistent Situation Perception timeliness requirements vary for each command echelon. For example, timeliness needs can be as long as months for the National Command Authority or Commanders-in-Chief and as short as seconds for unit commanders. The Consistent Situation Perception architecture must be a global information processing and display network that will:

- C Connect and focus all sensors for a given geographical area or battlespace;
- C Allow access to relevant databases at all available security levels that may provide information on the status, capabilities, or intentions of platforms/units of interest;

- Provide a flexible display and user interaction capability to tailor information easily and quickly to users' specific interests, desired level of detail, and terminology.

The thrusts of this initiative are:

- Deployable, fixed and mobile, manned and unmanned surveillance, reconnaissance, and intelligence systems;
- Real-time management of surveillance, reconnaissance, and intelligence systems;
- Real-time understanding of and adaptation to the environment and geopolitics;
- The use of surveillance, reconnaissance, and intelligence systems in nontraditional roles;
- The use of non-Navy, non-DoD systems to support consistent situation perception;
- Provide mechanisms for determining the status and intentions of all units in the area of interest;
- Fusing disparate surveillance, reconnaissance, and intelligence data to produce the picture;
- Ground truthing of the resulting perception.

The two fundamental Consistent Situation Perception objectives are to create a timely situation perception and to make it consistent and understandable at all levels within each user community.

The importance of Consistent Situation Perception was identified in the CINCs' future technical needs statements. They cited:

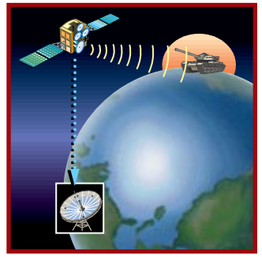
For *joint strike warfare*—"Current systems cannot collect and fuse all-source tactical information from Navy, Joint, Allied and Coalition sources. This results in a foggy overall tactical picture. All elements of this picture, including primary collection, fusion and dissemination architectures, deconfliction, classification, broadcast, and display technologies, are critical. The architecture for pulling this picture together is a major system engineering challenge, and should include all sensor platforms (air, surface, submarine and space) and two-way information sharing. Any such system must be reliable, robust, and secure for effective command and control. Naval forces cannot play in the joint arena without it....."

For *joint littoral warfare*—"A system which facilitates a common/consistent joint, combined or coalition tactical picture is required. It should possess the ability to fuse all-source data, have multi-level security (including the ability to selectively pass information to different operational partners), and allow two-way transfer of information (e.g., from Navy units to Joint Task Force units). Above all, it should respond in tactical time frames."

Consistent Situation Perception Evolution

Today... Evolving to... → TOMORROW

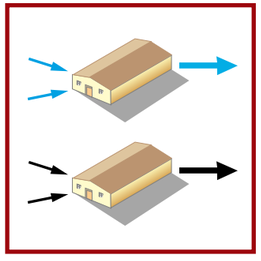
Sensors



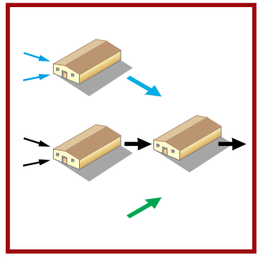
- Platform-based and single-spectral sensors
- Sensors designed for and highly effective against today's air threats
- Limited counter-C^3 capability

- Deployable multispectral sensor suites
- Sensors for reduced cross-section targets
- Integration of artificial intelligence/neural net technology with sensors
- Obliquely looking optical sensors for tactical aircraft
- Transportable sensors
- Exploiting commercial technology

Fusion

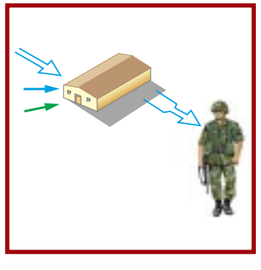


- Multiple independent fusion systems
- Limited integration (sensor type diversity; service/organic boundaries; warfare areas)

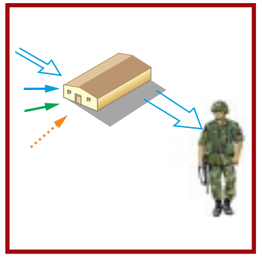


- All-source sensor fusion
- Fusion with allied and commercial sources
- Integration with combat and C^2 systems
- Multilevel security for sources and products, with sanitization
- 3-D and virtual reality techniques for display and interaction
- Battle damage assessment information fusion

Dissemination



- Sensor data and fused product translators for interoperability
- Low capacity available for sensor data and product dissemination



- Interoperable common formats and vernacular for sensor data and fused products
- Low-detectability connectivity for deployed sensor systems
- High-capacity connectivity for sensor data and fused product distribution

Collaborative Planning

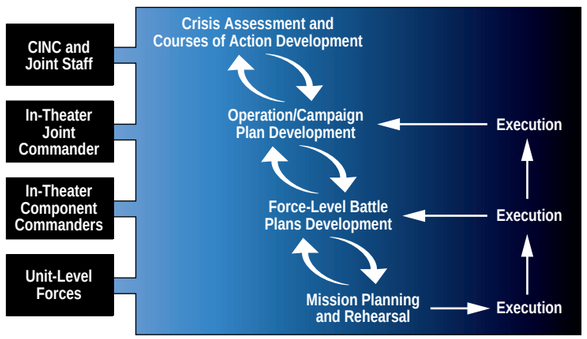
The Collaborative Planning initiative focuses on how to use a common understanding to gain military advantage. Starting with a consistent situation perception, warriors who have superior information in specific aspects can discuss options with each other before committing forces to action. Displays of diverse information are needed, as well as the capability to access selected information and hold remote discussions among distributed users. A capability for distributed modeling and simulation provides clearer descriptions of potential results of different military options. Our challenge is to provide user-transparent methods for information manipulation by users who have a common high-level goal but who have diverse lower level tasks.

Collaboration enables groups to coordinate unique, individual abilities for collective problem solving or plan development. Distributed collaboration implies that individuals may be in physically separate locations. Effective collaboration produces a collective product better than what could be produced by the participants separately; often this can also be achieved in less time. In C4I, collaboration is useful for situation assessment, planning, and coordinated execution of a plan. The latter collaboration category is usually called “synchronized battle management” or “synchronized execution.”

Effective collaboration produces a collective product better than what could be produced by the participants separately; often this can also be achieved in less time.

The Joint Planning and Execution Process

Planning proceeds from the levels of a Theater Commander-in-Chief (assessment and options), through the Joint Task Force Commander (campaign planning) and Joint Task Force Component (daily battle planning), to the unit (mission). At each step, plans are refined and coordinated with objectives and limits across echelons and missions.

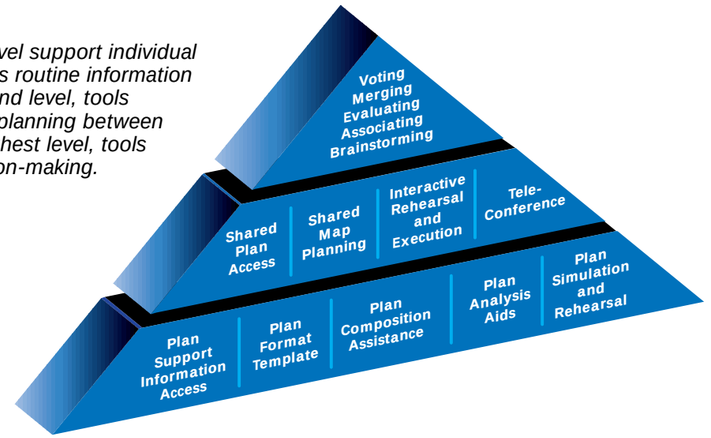


For joint/naval warfare, Collaborative Planning must consider a medium time frame for crisis planning and response before engagement (typical theater/Joint Task Force-level planning) and before tactical engagement or noncombat actions. This differs from ongoing “deliberate planning” collaborations on standing warplans at annual meetings for plan updates. With fewer chances of global conflict and more chances of spontaneous regional conflicts, there is less reliance on a deliberate planning process. Collaboration in the two processes needs different participants and communications. In the near term, these differences may limit the degree of collaboration (e.g., tactical forces are now limited to naval messages, voice circuits, and tactical data links), but the long-term goal is seamless extension of all-force collaboration.

Collaboration tools for warfighters are at three levels. Tools at the lowest level make individual planning jobs easier (e.g., laptop computers help with routine jobs for handling information); productivity is aided by access to consistent (across planners) supporting information relevant to current tasks. Second-level collaboration tools help coordinate distributed individuals to plan or execute their roles (e.g., plan updates exchanged between a J3/N3 organization and J4/N4 support planners; situation changes announced by J2/N2). Ideally, this collaboration level provides both information sharing and alerts to planners and warfighters when underlying information, goals, or assumptions of their own plan are changed by support planners.

Three Levels of Collaborative Planning Tools

Tools at the lowest level support individual planning jobs, such as routine information handling. At the second level, tools support coordinated planning between individuals. At the highest level, tools support group decision-making.

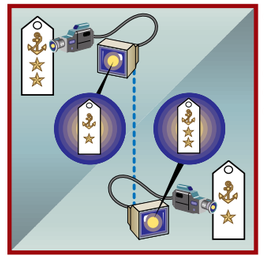


The highest collaboration level uses tools for group decision-making. Not all aspects of planning and execution need this level of collaboration. Many military operations are a top-down process of successive refinement and coordinated feedback. Group decisions are useful for situation assessment (when information is incomplete or contradictory and perspectives vary among participants) and evaluation (optimization among courses of action). Group decision-making for execution is less frequent, but may focus on collective assessment of differences between current operations and plans (vice simple plan repair). Effective team decision-making includes tools to force consideration of differing perspectives, weight decision aspects by importance, and encourage full active participation.

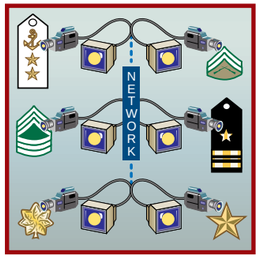
Distributed Collaborative Planning Evolution

Today... Evolving to... TOMORROW

Collaboration Media

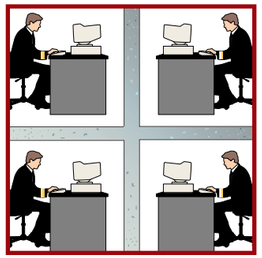


- Admiral-level video conferencing; compressed quality
- White-boarding
- Static maps
- Exchange of plans and plan objects

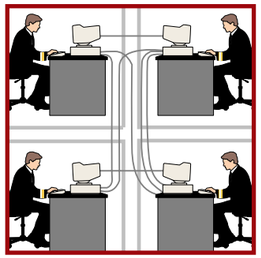


- Warrior-level video conferencing; full-motion available
- Dynamic map objects
- Compressed delta update of plans and plan objects

Collaboration Applications

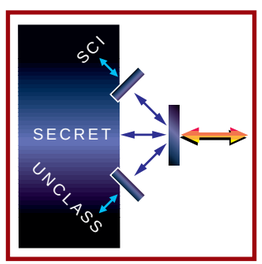


- Schedule promulgation
- "Job" scheduling



- Automated schedule change propagation
- Parallel scheduling

Connectivity Technology



- System-high security
- Secure capacity limitations on media

- Multilevel security
- High-capacity connectivity for collaboration

Information Warfare

Today, many nations, particularly the United States, rely heavily on information technology to gain information dominance. That reliance makes information systems an attractive target if appropriate weapons are available. Increasingly, potential adversaries can attack data (information) within databases, computers, communications links, and sensors. Information systems are vulnerable. For dominance in the information domain, we must protect our own information resources and be prepared to both affect and exploit an enemy's. If we can effectively exploit, deny, disrupt, or destroy information available to the enemy's forces, we can affect the adversary's situation perception and options in ways that can reduce conflict and speed peacemaking. The Information Warfare initiative focuses on ways to protect our information resources while denying our enemy the information needed to implement aggressive actions.

In response to the challenges posed by the increasing power of information and information systems, information warfare is emerging as a major new area of conflict. The Office of the Assistant Secretary of Defense (C^3I) has defined information warfare as "actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks." Information warfare includes military deception; destruction, denial, and exploitation of information; and information security. Information warfare seeks to preserve the integrity of the information we use for decision-making, while at the same time exploiting and affecting an adversary's information, and thus his understanding and decisions.

The required capabilities for conducting *military deception* include the ability to:

- C Generate a believable set of interrelated events;
- C Evaluate the impact of the information warfare plan on own and adversary's performance;
- C Coordinate and plan information warfare across the continuum of command and agencies;
- C Predict the relationship between information and behavior;
- C Control information in the military infosphere.

Information resides in the electronic infosphere. Techniques are needed for *destruction, denial, and exploitation of information* in this space. Required capabilities include the ability to:

- C Identify the adversary's infosphere vulnerabilities;
- C Attack the vulnerabilities with soft- and hard-kill weapons;
- C Resolve legal and ethical issues on the application of infosphere weapons.

Information is a precious commodity. Militarily, we want to keep our perceptions, plans, and capabilities secret until we are ready to release them. Economically, we want to keep our technological knowledge out of the hands of our competitors. Today, much information resides in a shared international infrastructure, with the military relying more than ever before on this unclassified reservoir. The vulnerabilities that we identify in the threat are also our vulnerabilities. Even when some information is considered to be proprietary by the military, the delivery and processing systems are likely to be based on commercial products. We are as vulnerable as our weakest link. Required capabilities for *information security* include the ability to:

- Conduct risk assessments;
- Detect and control intrusions and misuse;
- Secure information and also selectively share it.

Information warfare seeks to preserve the integrity of the information we use for decision-making, while at the same time exploiting and affecting an adversary's information, and thus his understanding and decisions.

Information warfare is conducted at all levels. It can be an alternative to conventional, destructive warfare and can redefine the nature of hostile acts among nations. In conventional, destructive warfare, information has become the critical commodity of war. Tactical information warfare sustains our information flow while reducing the quality of the "threat's" information flow. Tactical information warfare creates the battlespace and killing zone to send the right weapon to the right target at the right time. Today, information is a key element of the battlespace. The battlespace for the first time in history includes a complete abstraction. In an information war, the killing zone is where you choose to set it up, with every point in the infosphere a potential launch point.

Information warfare might be described in the terms of goals, tools, capabilities, and transformations. The goals are to protect, attack, exploit, and operate. The tools are those of Command and Control Warfare and C^4I: operations security (OPSEC), military deception, psychological operations (PSYOPS), electronic warfare (EW), physical destruction, and C^4I. The system support capabilities are the sensor, communication, and weapon grids. The "information" transformations are from data collection, to information, to knowledge, to understanding, and finally to plans and execution.

The other four corporate initiatives call out technologies that will enhance our abilities to transform data to understanding and execution in support of achieving our information warfare goals. These same technologies that allow us to more effectively use information are also our information warfare vulnerabilities. Examples of both supporting and vulnerable technologies from the other initiatives are:

- PCS/pager/cellular wireless individual communications
- Multimedia and virtual reality
- Knowledge robots and intelligent agents
- Commercial technology
- Fusion with allied and commercial sources of data/information
- Delta update of plans and plan objects

What these technologies have in common is the power to modify understanding or precisely match information with individual user requirements. The tactical information warfare goals—exploit, attack, protect, and operate—are achieved by our ability to enhance our understanding and information-manipulating capabilities in a precisely controlled fashion. Today, technology lets us see in the dark; tomorrow, technology may help us "see" into our adversary's thinking process. Today we can precisely guide a missile through a target window hundreds of miles away; tomorrow we may be able to target an information warfare weapon just as precisely. Today we can build firewalls around important information systems; tomorrow we may be able to inoculate software objects against viral attacks.

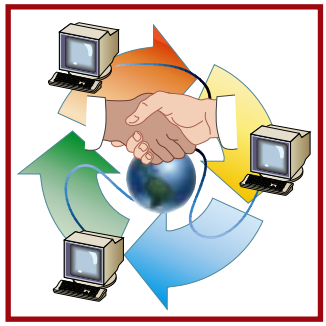
The weakness of these technologies is the ease with which data, information, and knowledge can be corrupted, and the difficulty in verifying the accuracy of the data. The new information technologies allow for the creation of artificial abstract worlds (our "understanding") that can be internally consistent but that lack simple ties to the raw sensor data on which they are constructed. A challenge in developing and fielding new information technologies is for us to garner the advantages in improved C^4I while mitigating the potential for these capabilities to be used against us.

Information Warfare Evolution

Today... Evolving to... TOMORROW

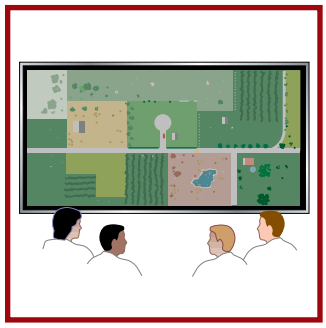
Protect

- Link encryption
- Red ship concept
- Firewalls

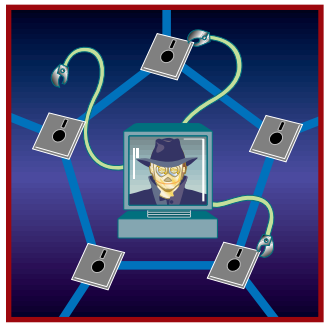


- Multilevel secure distribution and release of information
- Database and software encryption and authentication
- Intrusion diagnosis and alerting
- Intrusion recovery

Exploit

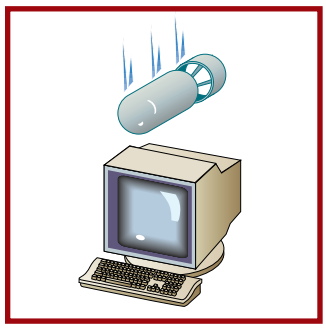


- Imagery
- Human intelligence
- Signals exploitation
- Manual review of open sources

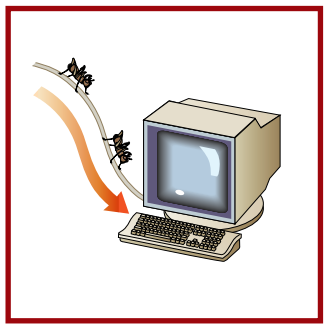


- Software information collection and fusion knowbots
- Covert unmanned sensors
- Battle Damage Assessment and intelligence integrated into the sensor grid

Attack

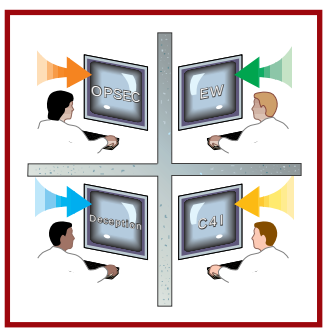


- Command training and experience
- Deceptions exterior to adversary C4I (e.g., feints and maneuver)
- Case-by-case (ad hoc) implementation

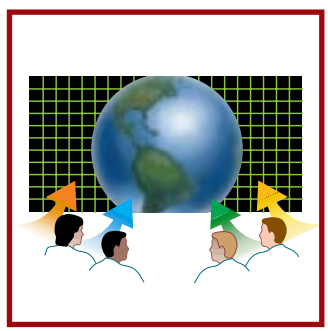


- Adversary decision modeling and simulation
- Information decoy and C4I deception devices
- Precision guided information destruction weapons
- Doctrine integration for tactics and technology

Operate



- No current career path for Command Control Warfare Commander, so few experts
- Few, and stand-alone, decision support tools



- Electronic collaboration across agencies, echelons, and expertise
- Visualization of diverse Command Control Warfare tools and effects
- Integrated C4I and Command Control Warfare Commander—an Information Warfare Specialist
- Integrated information warfare system

NRaD, the RDT&E Division of the Naval Command, Control and Ocean Surveillance Center (NCCOSC), provides a full range of customer services, from research, development, test, and evaluation (RDT&E) to direct Fleet support and in-service engineering.

For more information on NRaD programs and facilities, please contact us. We welcome your inquiries.

COMMANDING OFFICER
ATTN PUBLIC AFFAIRS OFFICE
NCCOSC RDTE DIV
53560 HULL ST
SAN DIEGO, CA 92152–5001

Reviewed and approved by
Executive Officer
NCCOSC RDT&E Division

TD 2890
June 1996

A Product of the Technical Information Division (TID)